



H-ISAC®

HEALTH - ISAC



Meeting the Challenge! — An Overview of 2021

After SolarWinds at the end of 2020, who ever imagined that 2021 would continue the spin on the hamster wheel? ProxyLogon, Accellion, PrintNightmare, VPN vulnerabilities in Fortinet, Pulse and Citrix, Colonial Pipeline, JBS Meats, Irish National Health Service, Kaseya and Log4j were just some of the headlines that kept us all spinning.

A recent Redscan analysis of the National Vulnerability Database (NVD) revealed a record 18,439 vulnerabilities were disclosed.

That’s not to mention an alarming trend of physical and cyber attacks on vaccine development and distribution as well as healthcare staff. And a disturbing rise in geopolitical rhetoric. Will 2022 break even more records?

At Health ISAC, the community continued its successful efforts to gather facts, analyze impacts and share best practices and mitigation strategies. We added over 100 new member organizations to the sharing community bringing the number of connected security professionals around the world to over 5,500. We fortified the community with new tools such as a new automated threat indicator sharing platform - Health Indicator Threat Sharing platform (HITS) and connected Members within our new threat intelligence portal.

In 2021 the Health ISAC Threat Operations Center (TOC) augmented *Monthly Member Threat Briefings* with 149 *Finished Intelligence Reports*, over 379 *Targeted Alerts*, 10 *TOC Spotlight* threat and vulnerability webinars, and distributed over 57,328 high fidelity indicators of compromise. New for the year were *Continue the Conversation* webinars for Members to bring subject matter expert panels to hot topic conversations from the chat channels.

We connected Members to each other through nine customized exercises, the Hobby Exercise, an Analytics Training Workshop, and three global in-person Summits, with our Fall Summit attendance close to pre-pandemic numbers. Health-ISAC committees and working groups produced four white-papers, a Pharma and Supply Chain Guidance for practitioners and healthcare CISOs, and expanded physical threat information deliverables for Health sector organizations.

And we are positioning and strengthening the ISAC itself to allow for even more capabilities in the future with more staff and expertise, technology and planning such as strategic, crisis management and succession plans.

I’m looking forward to working with the community to meet whatever challenges 2022 will bring!

Sincerely,

Denise Anderson

Health-ISAC President and CEO

Top Health Related Cyber & Physical Events for January:

[Log4j Attackers Switch to Injecting Monero Miners via RMI](#)

[Microsoft December 2021 Patch Tuesday Fixes 6 Zero-Days, 67 Flaws](#)

[55 People Arrested at Third Brussels Anti-Vax Protest](#)

[Kronos Ransomware Attack May Cause Weeks of HR Solutions Downtime](#)

[Hackers to Start Pushing Malware in Worldwide Log4Shell Attacks](#)

[Emotet Now Drops Cobalt Strike, Fast Forwards Ransomware Attacks](#)

[Federal Jury Convicts Pharmacy Owner for Role in \\$174 Million Telemedicine Pharmacy Fraud Scheme](#)

[AWS US-East-1 Outage Brings Down Services Around the World](#)

[Sabbath Ransomware Targeting Healthcare, Mandiant Warns](#)

[FBI: Cuba Ransomware Breached 49 US Critical Infrastructure Orgs](#)

H-ISAC is pleased to publish a monthly member newsletter. It is designed to bring events and other important ISAC information to your attention. If there is something you would like to see included please email:

contact@h-isac.org



@H-ISAC



@HealthISAC



@Health-ISAC

Product Security Updates
Apache Log4j (CVE-2021-44228)
Updated December 22, 2021

PRODUCT SECURITY UPDATES:Log4j

Log4j was developed by the Apache Foundation and is widely used for logging purposes.

H-ISAC in conjunction with the Threat Intelligence Committee has distributed a number of alerts and information for members and the public where applicable.

In addition we've created a 'one-stop shop' for companies to understand impacts to medical devices.

Go to <https://h-isac.org/apache-log4j-notices/> to learn more.

Quicklinks



Abbott is aware of the recently discovered remote code execution vulnerability impacting Apache Log4j, a logging tool commonly used in Java-based software applications.

Our cybersecurity team is actively evaluating our products, systems and applications to determine if there is any potential impact from this vulnerability and taking steps to mitigate any possible exposure.

Based on our analysis to date, none of our products are currently vulnerable. However, we will continue to analyze and monitor all available information and provide updates to our customers if needed.

[View](#)



B. Braun

B. Braun's first analysis determined that NONE of our software products are affected.

[View](#)



Baxter

Please note that the Apache Log4j vulnerability is not a Baxter-specific vulnerability. As part of the company's product security policy and protocols, Baxter steams evaluating Baxter's Java based products and solutions for potential impacts from this reported vulnerability and

UPCOMING SUMMITS



APAC Summit!

Be part of this great event. H-ISAC is seeking dynamic speakers with thought provoking presentations. Share

case studies, lessons learned, real time strategies or current challenges with leaders in the global healthcare community.

Submit a brief abstract and title today!

<https://h-isac.org/summits/inaugural-apac-summit-2022/>



Mark your calendars for the upcoming **Spring Americas Summit.**

Better yet, **participate** in the May Health-ISAC Summit in Orlando as a presenter.

Be part of the *Ohana Village* family by sharing your recent success or lessons learned story with your family of healthcare security peers.

Submit a brief abstract and title today!

<https://h-isac.org/summits/spring-2022-summit/>

COMMUNITY SERVICES SPOTLIGHT

Health-ISAC Community Services



API attacks are predicted to become the subject of more attacks in 2022. APIs are crucial to business and keep you connected to your customers. Salt offers API protection. Salt uses ML and AI to help identify all your APIs, stop an attack in its early stages, and compile insight on how to strengthen API security against future attacks.

Exclusive H-ISAC Member offers from Salt:

- A complementary API security risk analysis
- 15-months for the price of 12

Learn more here: <https://h-isac.org/community-services/#salt>

Pharma and Supply Chain

For Practitioners and CISOs

The Pharma & Supply Chain Working Group recently developed a pharmaceutical supply chain security framework for Health-ISAC Members. There are two components to the framework:

1. **Practitioners Guide** – an interactive document that provides the framework controls and offers perspectives around specific supply chain security issues in Third Party, IT, and OT Security.
2. **Securing The Modern Pharmaceutical Supply Chain (CISO Leadership Guide)** – provides a perspective from the leading pharma CISOs on the importance and implementation strategies necessary to successfully implement a Supply Chain Security strategy.

Health-ISAC Members can email contact@h-isac.org to request access to the guides.

UPCOMING EVENTS — Or visit our Events Page <https://h-isac.org/events/>

Health-ISAC Navigator webinar

SASE for the Connected Health Ecosystem
by
Palo Alto Networks

Tuesday, January 11
1:00pm ET

<https://h-isac.org/hisacevents/sase-for-the-connected-health-ecosystem-by-palo-alto-networks/>

Health-ISAC Navigator webinar

Measuring Healthcare and Hospital Cybersecurity
by
BitSight

Tuesday, January 18
2:00pm ET

<https://h-isac.org/hisacevents/measuring-healthcare-and-hospital-cybersecurity-performance-by-bitsight/>



Health-ISAC Monthly Member Threat Briefing TLP AMBER

Tuesday, January 25
12pm ET

<https://H-Isac.Org/Hisacevents/H-Isac-Monthly-Member-Threat-Briefing-January-25-2022/>

Health-ISAC Partnered Event

2022 National ResilienceExch Virtual Summit January 25-27

Building Resilience: ISAC Lessons Learned in 2021
panel moderated by
H-ISAC President / CEO

Tuesday, January 25
12:30pm ET

<https://h-isac.org/hisacevents/2022-national-resilienceexch-virtual-summit/>